IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Re:	Application of:	Rhodes et al.
	Serial No.:	10/671,234
	Filed:	September 25, 2003
	For:	Ethernet-Based Fire System Network
	Group Art Unit:	2446
	Confirmation No.:	8197
	Examiner:	Benjamin R. Bruckart
	Our Docket No.:	2003P14811US (1867-0039)

BRIEF ON APPEAL

Sir:

This is an appeal under 37 CFR § 41.31 to the Board of Patent Appeals and Interferences of the United States Patent and Trademark Office from the rejection of claims 1-20 of the above-identified patent application. Claims 1-20 have been finally rejected in an Office Action dated February 1, 2010. Applicants previously submitted a fee of $540.00 in connection with an Appeal Brief filed June 8, 2009. An Office Action mailed August 17, 2009 reopened prosecution after the June 8 Appeal Brief was filed to apply a new grounds of rejection. Applicants respectfully request that the previously submitted fee of $540.00 for the June 8, 2009 Appeal Brief be applied toward the present Brief on Appeal. Also, please provide any extension of time which may be necessary and charge any fees which may be due to Deposit Account No. 19-2179, but not to include any payment of issue fees.

(1) REAL PARTY IN INTEREST

Siemens Building Technologies, Inc. is the owner of this patent application, and therefore the real party in interest.

(2) RELATED APPEALS AND INTERFERENCES

There are no related appeals or interferences in this case.

(3) STATUS OF CLAIMS

Claims 1-20 are pending in the application.

Claims 1-20 stand rejected and form the subject matter of this appeal.

Claims 1-20 are shown in the Appendix attached to this Appeal Brief.

(4) STATUS OF AMENDMENTS

Appellants filed no amendments subsequent to the final rejection contained in the Office Action mailed February 1, 2010 (hereinafter "Final Office Action").

(5) SUMMARY OF THE CLAIMED SUBJECT MATTER

I. Independent Claim 1

Independent claim 1 is directed to a "data transmission system for a facility". With reference to the specification, e.g., at pages 17-18 and the drawings, e.g., FIGS. 3, 5, and 6, claim 1 recites "*a first network*". An exemplary "first network" is the fire control network 100 shown in FIGs. 5 and 6 and described at page 17, lines 7-23 of the specification. [*Also*

see fire control network 10 of FIG. 3, with reference to page 18, line 23 to page 19, line 13 of the specification.]

Claim 1 also recites "*a number of critical devices disposed within the facility*". The "critical devices" may be fire control devices, such as those shown in FIG. 1, and described at page 12, line 18 to page 13, line 12 of the specification. For example, the fire control devices may include initiating devices (such as smoke detectors 22 and pull switches 24) and notification devices 26 (such as horns, strobes or speakers). [*Also see* IDC and NAC devices in FIG. 3.]

Claim 1 includes the further limitation of "*at least one first computer workstation operably coupled to said number of critical devices via said first network*". The "computer workstations" are shown in FIGs. 5 and 6 as fire control workstations 102 and 104. These fire control workstations 102 and 104 are described in the specification at page 17, lines 7-23. Further information concerning the fire control workstations can be found in the specification at page 10, line 21 to page 12, line 17, describing fire control workstations 12 and 13 of FIG. 1. [*Also see* fire control workstation 52' of FIG. 3, with reference to page 19, lines 3-11 and page 22, lines 3-17.]

Claim 1 also recites "*a second network including at least one second computer workstation*". "A second network" is shown in FIG. 6 as reference numeral 216, which includes a corporate network 218. "At least one second computer workstation" is shown in FIG. 6 by building control workstations 212 and 214. As explained at page 14, line 5 to page 15, line 15 of the specification, the building control workstations may be those that implement building automation software for a building automation network such as a network that controls the overall building environment by managing air handlers that supply

heated or cooled air to a building. [*Also see* corporate network 75 and non-fire related workstation 71 in FIG. 3, with reference to page 20, lines 12-14 and page 22, lines 6-17.]

Finally, claim 1 recites "*an isolating router coupling said first network to said second network and operable to isolate said first network from data transmission traffic in said second network, the isolating router comprising a router configured to receive and store data packets, and to forward the received data packets*." An example of such an "isolating router" is shown in FIG. 6 as reference numeral 224, and described at page 18, lines 7-18 of the specification. [Also see IP router 72 of FIG. 3, with reference to page 22, lines 6 to page 23, line 21.]

II. Independent Claim 8

Independent claim 8 is directed to a "data transmission system for use in a facility." As shown in FIG. 3, the data transmission system comprises a first fire control Ethernet sub-network (10, 14) including a number of fire control devices (IDC, NAC, etc.). A number of fire safety workstations (52', 54') are operably coupled to said fire control devices and operable to implement software for maintaining and controlling said fire control devices (*see* p. 22, lines 5-20 of the specification).

FIG. 3 also shows a second building control Ethernet sub-network (50) including a number of building control devices (50, including TECs and UCs) and a number of building automation workstations (71) operably coupled to said building control devices (50) and operable to implement software for maintaining and controlling said building control devices (*see* p. 14, line 17 to p. 15, line 3 of the specification).

FIG. 3 also shows an isolating IP router (72) connecting said first sub-network to said second sub-network and operable to isolate said first network from data transmission traffic in said second network (*see* p. 22, lines 6-12 of the specification).

III. Independent Claim 14

Independent claim 14, is directed to a data communication system for a facility. As shown in FIG. 3, the data communications system comprises a first network (10) and a second network (75) connected by an IP router (72). The first network (10) including a first plurality of work stations (52', 54') and the second network (75) including a second plurality of work stations (via 75). The first plurality of workstations include only building system workstations (52', 54'), and the second plurality of work stations include only non-fire safety related building system workstations and non-building system workstations (*see* p. 23, lines 9-15). The IP router (72) enables communication between the non-fire related building system workstations (via 75) and the first plurality of workstations (52', 54'). The IP router is also operable to disable communication between the non-building system workstations (via 75) and the first plurality of workstations (52', 54') (*see* p. 21, line 1 to p. 23, line 15).

(6) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 2, 7, and 14-17 have been rejected under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent Publication No. 2003/0023874 to Prokupets et al. ("Prokupets") in view of U.S. Patent No. 5,815,664 to Asano ("Asano").

Claims 3, 4, and 8-13 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Prokupets in view of Asano and further in view of U.S. Patent Publication

No. 2006/0114842 to Miyamoto et al. ("Miyamoto") in further view of U.S. Patent No. 6,144,736 to Koenig et al. ("Koenig").

Claims 5-6 and 20 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Prokupets in view of Asano in further view of Miyamoto.

Claims 18-19 have been rejected under 35 U.S.C. §103(a) as being unpatentable over Prokupets in view of Asano in further view of Koenig.

(7) ARGUMENT

I. The Rejection of Claims 1, 2, 7, and 14-17 under 35 U.S.C. §103(a) over Prokupets in view of Asano

Each of claims 1, 2, 7, and 14-17 stand rejected as being obvious over Prokupets in view of Asano. As explained below, however, the combination of Prokupets and Asano, as proposed by the Examiner, fails to arrive at the inventions of claims 1, 2, 7, and 14-17.

A. Independent Claim 1

The combination of Prokupets and Asano, as proposed by the Examiner, fails to arrive at a data transmission system in which a first network having a plurality of critical devices is coupled to a second network by an isolating router, as per claim 1.

1. Prokupets

Prokupets is directed to a system for integrating security and access for facilities and information systems. As shown in Fig. 1, the Prokupets system shows an access control system 22a, a surveillance system 22d, a fire system 22c, an intrusion detection system 22b, and information systems 18a-d. (See Prokupets at Abstract and Fig. 1). According to

Prokupets, "the security server 12 is connected to facility protection systems 22 and information systems 18, via a network 20, in which systems 18 and 22, and security server 12, each have an interface (hardware and software) enabling network communication. Network 20 represents any typical computer network, such as LAN, WAN, or Internet, in which each component in the network has an IP address." (Prokupets, para. [0021] and Fig. 1).

In addition, Prokupets discloses that the interface of the each of the systems 18 and 22 "is capable of receiving and sending data packets (records or files) to and from security server 12 via network 20." (Prokupets, para. [0027] and [0029]). The "security server 12 receives event data from systems 18 and 22, logs them in the central database 14, routes events to alarm monitoring clients and to the event transaction processor and then, depending on the event data, outputs action data packets (requests) to such systems 18 and 22, different from the system from which the event data is received, to take specific actions automatically and in real-time. The security server 12 may send in response to event data, messages to one or more output devices 16, such as automated calls to pagers, telephones, or e-mail, or other communication systems." (Prokupets, para. [0021]).

Thus, Prokupets discloses that the security system 12 is connected via an interface to a *single* network 20 to which the facility protection systems 22 and information systems 18 are also connected. In addition, Prokupets discloses a system in which all communications (i.e.., event data packets and action data packets) on the network 20 are directed to or received from the security server 12. There is no disclosure in Prokupets of any of the systems 18 and 22 directing packets to any of the other systems 18 and 22 via the network 20.

2. Asano

Asano is directed to an address reporting arrangement and method for detecting authorized and unauthorized addresses in a network environment. Asano addresses problems arising from a host computer having an authorized address trying to communicate with a host having an unauthorized address on another network. (See, e.g., Asano at col. 2, lines 53-59). It is the object of Asano to enable a host having an authorized address to respond to a request from a host having an unauthorized address. (*Id.* at col. 4, lines 26-38).

3. The Rejection of Claim 1

Claim 1 was rejected as being obvious over Prokupets in view of Asano. In rejecting claim 1, the Examiner cited the fire system 22c of Prokupets as corresponding to the first network having a number of critical devices disposed within a facility. (Final Office Action, page 2). Although a second network was not specifically referred to in the Final Office Action, the Examiner cited the alarm monitoring clients 24 of Prokupets as the at least one second computer workstation which in claim 1 is connected to a second network. Therefore, Appellants believe that the connection between the alarm monitoring clients 24 and the security server 12 is being cited as corresponding to a second network, as claimed in claim 1.

In addition, in the Response to Arguments section found on page 10 of the Final Office Action, the Examiner asserted the following:

> "Adding an isolating router to Prokupets would allow for data isolation between the HR database and the other devices such as the servers of tag 18a and 18c. HR database and HR Computer system are separate and data is only interfaced through the security server (tag 12). Therefore, the second network is isolated by functionality. (Final Office Action, Response to Argument section, page 10).

According to Prokupets, the Human Resource (HR) database 26 is accessible by the security server 12 through the Lightweight Directory Access Protocol (LDAP) protocol. (Prokupets, para. [0037]). In addition, Prokupets discloses that information system 18b corresponds to Lightweight Directory Access Protocol (LDAP) Server 18b. Consequently, Appellants believe that the Examiner is referring to the connection between the HR database 26 and the security server 12 via the LDAP Server 18b as corresponding to a second network, as claimed in claim 1, as an alternative or in addition to the "second network" between the alarm monitoring clients 24 and the security server.

The Examiner acknowledged that Prokupets fails to teach an isolating router that couples the first network (fire system 22c) and the second network (connection between HR database 26 and/or alarm monitoring clients 24 and LDAP server 18b). To provide the teaching of the isolating router, the Examiner cited Asano stating that it would have been obvious to modify the apparatus of Prokupets to include "an isolating router that processes packets as taught by Asano in order to selectively enable communication between different networks" (see Final Office Action, page 3).

In support of this contention, the Examiner stated the following:

> "By adding the isolating router of Asano to the Prokupets reference, you substitute or additionally add the common functionality and detailed features of the router to the security server to allow controlled data transmission between devices (Asano: coL 4, lines 25-33). The rationales of using a known technique to improve similar devices in the same way, applying a known technique to a known device ready for improve to yield predictable and similar results, combining prior art elements according to known methods to yield predictable results, and the TSM test as supported by KSR are fully supported by the combination of Prokupets with Asano. In a broader sense, one of ordinary skill in the art at the time of the invention, illustrate that router access and control between two networks are easily and readily borrowed, substituted, or applied to the Prokupets reference in order to selectively enable communication and addressing between different networks for access control (Asano: col. 4,

lines 25-33)." (Final Office Action, Response to Argument section, paragraph spanning pages 10 and 11).

Thus, the Examiner appears to be citing the security server 12 as coupling a first network, e.g. fire system 22c, to a second network, e.g., the connection between the security server 12 and alarm monitoring clients 24 and/or the connection between the security server 12 and the LDAP server 18b. Applicants respectfully submit, however, that, in either case, the Examiner has mischaracterized Prokupets.

4. Does Not Arrive at A First Network Coupled to A Second Network, as Claimed

Contrary to the Examiner's assertion, the security server 12 of Prokupets does not couple a first network to a second network. In particular, there is no disclosure in Prokupets of the security server 12 being connected to any other network than the network 20. As mentioned above, Prokupets discloses that the security server 12 has *an* interface for connecting to the network 20. Thus, the security server 12 sends and receives communications through its interface to the network 20. (Prokupets, para. [0021]).

Prokupets also discloses that each of the other systems 18, 22, 24 communicates with the security server 12 via the network 20. In particular, Prokupets discloses that the cited first network of Prokupets, i.e., the fire system 22c, sends and receives communications through an interface to the network 20. (Prokupets, paras. [0022] - [0027]). According to Prokupets, each of the information systems 18, including the LDAP server 18b (believed to be cited as corresponding to the second network of claim 1), also has an interface through which the respective systems receive and send data packets to and from the security server 12 via the network 20. (Prokupets, paras. [0028] and [0029]). Prokupets also discloses that the

alarm monitoring clients 24 communicate with the security server 12 over the network 20. (Prokupets, para. [0036]).

Thus, Prokupets discloses that each of the systems 18, 22, 24 as well as the security server 12 of Prokupets is connected to and communicates through a *single* network 20. There is no disclosure in Prokupets of a first network and a second network being coupled via the security server 12.

Moreover, claim 1 requires that the first network and the second network be coupled by an isolating router. As is generally familiar, a router is a specific type of device having two or more network interfaces for connection to two more different networks, and is configured to route data packets between the different networks by transferring packets from one interface to another based on source and destination addresses in the packets. As explained above, Prokupets discloses that the security server 12 has *an* interface for connecting to the network 20. There is no disclosure in Prokupets that the server 12 has a second interface or a separate interface for connecting to any other network, such as the fire system 22c or to the alarm monitoring clients 24. Therefore, the security server 12 is not capable of coupling two different networks in the same manner as a router, let alone in the same manner as the claimed isolating router.

Because the security server 12 of Prokupets is connected to a single network, a person of ordinary skill in the art would not be led to modify the security server 12 of Prokupets to include the functionality of "an isolating router that processes packets as taught by Asano in order to selectively enable communication between different networks", as asserted by the Examiner. Furthermore, such a modification would still not result in a coupling of a first network to a second network by an isolating router as claimed in claim 1.

5. No Reason to Modify Security Server with Router Functionality

In Prokupets, there is no disclosure of any communication being directed to the fire system 22c (first network of claim 1) via the network 20 by any of the other systems 18, 22, or 24. Consequently, there is no need to provide an isolating router for isolating the fire system 22c from data packets from the other systems 18, 22, and 24. All communications to the fire system 22c disclosed in Prokupets are from the security server 12 via the network 20. In fact, all communications disclosed in Prokupets are to and from the security server 12 via the network 20. Therefore, modifying the security server 12 to include the functionality of an isolating router, as claimed in claim 1, would only result in the capability of isolating each system, including the fire system 22c, from receiving data packets from the security server 12. Such a modification is clearly contrary to the teachings of Prokupets.

Furthermore, even if the security server 12 was connected between more than one network, it is respectfully submitted that a person or ordinary skill in the art would not be led to include the functionality of an isolating router in the security server 12 to route packets between networks because such functionality would limit the ability of the security server 12 to perform its intended function. For example, a router generally routes data packets from one network interface to another based on a limited amount of information regarding the packets, such as the input port, output port, or address information from the packets. The security server 12, however, is required to perform much more comprehensive processing of packets including storing event information contained in the packets, determining actions in response to event information, forwarding information to other devices, etc.. (Prokupets, see, e.g., para. [0011], [0034], [0039]).

Modifying the server 12 to include router functionality as taught by Asano would eliminate most of the information and data processing ability of the server 12. Processing event data and generating action data, however, is clearly one of the focal points of Prokupets. Therefore, it is respectfully submitted that the Examiner has not provided sufficient rationale or reasoning for why it would be obvious to modify the security server 12 to serve as an isolating router and potentially decrease or eliminate some or all of the functionality of the security server 12 in order to couple a first network and a second network.

6. Conclusion with Respect to Claim 1

In view of the foregoing, it is respectfully submitted that the combination of Prokupets and Asano, as proposed by the Examiner, fails to arrive at a data transmission system in which a first network having a plurality of critical devices is coupled to a second network by an isolating router. Accordingly, it is respectfully submitted that the obviousness rejection of claim 1 over Prokupets and Asano should be withdrawn.

B. Claims 2 and 7

Claims 2 and 7 also stand rejected as allegedly being obvious over Prokupets and Asano. Claims 2 and 7 depend from and incorporate all of the limitations of claim 1. As discussed above, the combination of Prokupets and Asano, as proposed by the Examiner, fails to arrive at the invention of claim 1. For at least these reasons, it is respectfully submitted that the obviousness rejections of claims 2 and 7 should be withdrawn as well.

C. Claim 14

Claim 14 is argued separately for the purposes of this appeal because it contains independent grounds for reversal not present in claim 1. Claim 14 also stands rejected as allegedly being obvious over Prokupets in view of Asano. Claim 14 includes the limitation of a first network and a second network being connected by an IP router. As explained above in connection with claim 1, the combination of Prokupets and Asano, as proposed by the Examiner, fails to arrive at a first and a second network connected by an IP router.

In contrast to claim 1, claim 14 also includes limitations directed to the first network including "*a first plurality of workstations*" that are only building system workstations. Contrary to the Examiner's contention, Prokupets fails to disclose a first network having a first plurality of workstations, as claimed in claim 14. To provide the teaching of the first plurality of workstations, the Examiner referred to Fig. 1 and para. [0024] of Prokupets. Para. [0024] of Prokupets, however, is directed to the fire system 22c and discloses that the fire system 22c includes fire panels capable of controlling operation of the fire system 22c. However, there is no mention in paragraph [0024] of the fire system 22c including a plurality of workstations, and the Examiner has not provided any rationale for why it would be obvious to equate the fire panels of the fire system 22c to building system workstations as claimed in claim 14.

Accordingly, in addition to the reasons given above in connection with claim 1, it is respectfully submitted that the combination of Prokupets and Asano, as proposed by the Examiner, fails to arrive at a first and a second network in which first network includes a plurality of only building system workstations, as claimed in claim 14. Therefore, it is

respectfully submitted that the obviousness rejection of claim 14 over Prokupets and Asano should be withdrawn as well.

D. Claims 15-17

Claims 15-17 also stand rejected as allegedly being obvious over Prokupets and Asano. Claims 15-17 depend from and incorporate all of the limitations of claim 14. None of the modifications of Prokupets and Asano proposed in connection with claims 15-17 cures the deficiencies of Prokupets and Asano with respect to claim 14. Accordingly, for at least the same reasons as given for claim 14, it is respectfully submitted that the obviousness rejection of claims 15-17 over the Prokupets and Asano should be withdrawn as well.

E. Additional Reasons for the Patentability of Claim 16

Claim 16 is argued separately from claim 14 for the purposes of this appeal because it contains independent grounds for reversal not present in claim 14. For example, claim 16 includes the limitation that "the first plurality of workstations includes at least one fire safety system workstation and at least one non-fire building system work station." The Examiner referred to the fire system 22c as corresponding to the first plurality of workstations. However, there is no disclosure in Prokupets of the fire system 22c including non-fire building system workstations. Therefore, it is respectfully submitted that claim 16 has additional reasons for patentability over the combination of Prokupets and Asano.

III. The Rejection of Claims 3, 4, and 8-13

Claims 3, 4, and 8-13 were rejected as being obvious over Prokupets in view of Asano in further view of Miyamoto and Koenig. As explained below, the combination of Prokupets, Asano, Miyamoto, and Koenig, as proposed by the Examiner, fails to arrive at the inventions of claims 3, 4, and 8-13.

A. Claims 3 and 4

Claims 3 and 4 depend from and incorporate all of the limitations of claim 1. As discussed above, the combination of Prokupets and Asano, as proposed by the Examiner, fails to arrive at the invention of claim 1. The modifications of Prokupets and Asano with Miyamoto and Koenig proposed in connection with claims 3 and 4 do not cure the deficiencies of Prokupets and Asano with respect to claim 1. Therefore, for at least the same reasons as given for claim 1, it is respectfully submitted that the obviousness rejections of claims 3 and 4 should be withdrawn as well.

B. Claims 8-13

Claims 8-13 also stand rejected as allegedly being obvious over Prokupets, Asano, Miyamoto and Koenig. Independent claim 8, however, is directed to a data transmission system which includes limitations directed to "a first fire control Ethernet sub-network including a number of fire control devices" and "a second building control Ethernet sub-network including a number of building control devices" connected by "an isolating IP router" operable to isolate said first network from data transmission traffic in said second network. As discussed above in regard to claim 1, the combination of Prokupets and Asano,

as proposed by the Examiner, fails to arrive at a data transmission system in which a first network is coupled to a second network by an isolating router, nor do the modifications of Prokupets and Asano with Miyamoto and Koenig proposed in connection with claims 8-13 cure the deficiencies of Prokupets and Asano with respect to claim 1. Accordingly, it is respectfully submitted that the obviousness rejection of claims 8-13 over Prokupets, Asano, Miyamoto, and Koenig should be withdrawn as well.

IV. The Rejection of Claims 5, 6 and 20

Claims 5, 6 and 20 were rejected as being obvious over Prokupets in view of Asano in further view of Miyamoto. Claims 5, 6 and 20 depend from and incorporate all of the limitations of claim 1. As discussed above, the combination of Prokupets and Asano, as proposed by the Examiner, fails to arrive at the invention of claim 1. The modifications of Prokupets and Asano with Miyamoto proposed in connection with claims 5, 6 and 20 do not cure the deficiencies of Prokupets and Asano with respect to claim 1. Therefore, for at least the same reasons as given for claim 1, it is respectfully submitted that the obviousness rejections of claims 5, 6 and 20 should be withdrawn as well.

V. The Rejection of Claims 18 and 19

Claims 18 and 19 were rejected as being obvious over Prokupets in view of Asano in further view of Koenig. Claims 18 and 19 depend from and incorporate all of the limitations of claim 14. As discussed above, the combination of Prokupets and Asano, as proposed by the Examiner, fails to arrive at the invention of claim 14. The modifications of Prokupets and Asano with Koenig proposed in connection with claims 18 and 19 do not cure the

deficiencies of Prokupets and Asano with respect to claim 14. Therefore, for at least the same reasons as given for claim 14, it is respectfully submitted that the obviousness rejections of claims 18 and 19 should be withdrawn as well.

VI. CONCLUSION

For all of the foregoing reasons, claims 1-20 are not unpatentable under 35 U.S.C. § 103(a). As a consequence, the Board of Appeals is respectfully requested to reverse the rejection of these claims.

Respectfully submitted,

/Thomas J. Burton/
Thomas J. Burton
Attorney for Applicants
Attorney Registration No. 47,464

July 1, 2010

Siemens Industry Inc.
Law and Patent Department
1000 Deerfield Parkway
Buffalo Grove, IL 60089
Phone: 847-941-6823
Fax: 847-941-6810

(8) CLAIMS APPENDIX

1. A data transmission system for a facility comprising:

a first network including;

a number of critical devices disposed within the facility;

and at least one first computer workstation operably coupled to said number of critical devices via said first network;

a second network including at least one second computer workstation; and

an isolating router coupling said first network to said second network and operable to isolate said first network from data transmission traffic in said second network, the isolating router comprising a router configured to receive and store data packets, and to forward the received data packets.

2. The data transmission system of claim 1, wherein:

said first network is a fire control network;

said number of critical devices include fire control devices; and

said first computer workstation implements software configured to receive data from and transmit data to said fire control devices.

3. The data transmission system of claim 2, wherein said first network includes a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses and that is operable to electrically isolate said first network from said isolating router.

4. The data transmission system of claim 1, wherein:

said first network includes a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses and that is operable to electrically isolate said first network from said isolating router; and

said isolating router meets one or more standards-issuing agencies publicly available standards for information technology equipment for fire protective signaling uses.

5. The data transmission system of claim 1, wherein said second network includes a building control network which includes a second Ethernet switch operably coupled to a number of building control devices independent of said operationally critical devices.

6. The data transmission system of claim 5, wherein:

said second network includes a corporate network, independent of said building control network, which includes workstations capable of broadcast transmissions; and

said isolating router is operable to block said broadcast transmissions to said first network.

7. The data transmission system of claim 1, wherein:

said second network includes a corporate network, independent of said first network, which includes workstations capable of broadcast transmissions; and

said isolating router is operable to block said broadcast transmissions to said first network.

8. A data transmission system for use in a facility comprising:

a first fire control Ethernet sub-network including a number of fire control devices and a number of fire safety workstations operably coupled to said fire control devices and operable to implement software for maintaining and controlling said fire control devices;

a second building control Ethernet sub-network including a number of building control devices and a number of building automation workstations operably coupled to said building control devices and operable to implement software for maintaining and controlling said building control devices; and

an isolating IP router connecting said first sub-network to said second sub-network and operable to isolate said first network from data transmission traffic in said second network.

9. The data transmission system of claim 8, wherein said building automation workstations include a database server workstation and at least one database client workstation.

10. The data transmission system of claim 9, wherein database server workstation is connected within said first sub-network.

11. The data transmission system of claim 10, wherein all workstations connected within said first sub-network meet more standards-issuing agencies publicly available standards fire protective signaling uses than at least some workstations connected outside the first sub-network.

12. The data transmission system of claim 11, wherein said first sub-network includes a first Ethernet switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling uses.

13. The data transmission system of claim 12, wherein said isolating IP router meets one or more standards-issuing agencies publicly available standards for information technology equipment for fire protective signaling uses.

14. A data communication system for a facility comprising

a first network and a second network connected by an IP router, the first network including a first plurality of work stations, the second network including a second plurality of work stations, the first plurality of workstations including only building system workstations, the second plurality of work stations including only non-fire safety related building system workstations and non-building system workstations, and wherein the IP router enables communication between the non-fire related building system workstations and the first plurality of workstations, and the IP router is operable to disable communication between the non-building system workstations and the first plurality of workstations.

15. The data communication system of claim 14 wherein at least one building system work station is a fire safety system workstation connected to one of a plurality of fire safety system devices.

16. The data communication system of claim 14 wherein the first plurality of workstations includes at least one fire safety system workstation and at least one non-fire building system work station.

17. The data communication system of claim 14 wherein at least one of the non-fire building system workstations is operably connected to heating ventilation and air conditioning system devices.

18. The data communication system of claim 14 wherein the first network includes a switch that meets one or more standards-issuing agencies publicly available standards for fire protective signaling.

19. The data communication system of claim 14 wherein the IP router meets one or more standards-issuing agencies publicly available standards for information technology equipment for fire protective signaling.

20. The data communication system of claim 1 wherein the first network comprises at least one Ethernet network and the second network comprises at least one Ethernet network.

(9) EVIDENCE APPENDIX

[NONE]

(10) RELATED PROCEEDINGS APPENDIX

[NONE]